Le traçage comportemental des internautes sur les réseaux sociaux

Michel, Alejandra

Published in:
R.D.T.I.

Publication date:
2019

Document Version
le PDF de l'éditeur

Observations

Le traçage comportemental des internautes sur les réseaux sociaux : l'affaire des « cookies *Facebook* », véritable saga judiciaire ?

I. INTRODUCTION

Depuis 2015, l'affaire *Facebook*, opposant trois entités du réseau social[1] – américaine, irlandaise et belge – à l'ancienne Commission de la protection de la vie privée belge (ci-après « CPVP » ; et désormais devenue « Autorité de protection des données »), défraie la chronique. Pour cause, après une ordonnance de référé du président du tribunal de première instance néerlandophone de Bruxelles[2] et un arrêt de la cour d'appel de Bruxelles[3], le jugement commenté, rendu le 16 février 2018 par le tribunal de première instance néerlandophone de Bruxelles[4], constitue le premier jugement au fond dans ce que l'on peut appeler la « saga judiciaire » de l'affaire des « cookies *Facebook* ».

Pour rappel, à l'origine de cette affaire et après de nombreux échanges avec le service en ligne de réseaux sociaux, la CPVP a saisi le juge des référés pour dénoncer les techniques de traçages comportementaux (cookie « datr » et *social* plug-ins) utilisées afin de suivre les habitudes de navigation des internautes non inscrits sur *Facebook* se trouvant sur le territoire belge. En date du 9 novembre 2015, le président du tribunal de première instance néerlandophone de Bruxelles, relevant des manquements à l'ancienne loi du 8 décembre 1992 et à l'article 129 de la loi du 13 juin 2005, a donné raison à la CPVP[5]. En degré d'appel, l'ordonnance de référé a été réformée au motif, d'une part, que la Cour s'estimait sans compétence territoriale à l'égard des filiales américaine et irlandaise du groupe *Facebook* et, d'autre part, qu'à l'égard de l'établissement belge la demande était, à défaut d'urgence, sans fondement[6].

1 Il s'agit plus précisément de *Facebook Inc.* (États-Unis d'Amérique), *Facebook Ireland Limited* (Irlande) et de *Facebook Belgium SPRL* (Belgique).

2 Civ. Bruxelles (nl.) (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, n° 62, p. 91, note G. Dejemeppe. Pour une explication du phénomène de « pistage » mis en œuvre par les services de réseaux sociaux en ligne, voy. E. Degrave, « Facebook condamné par la justice belge : faut-il craindre d'être "pisté" ? », le 13 janvier 2016, disponible sur http://www.justice-en-ligne.be/article795.html, consulté le 10 janvier 2019. Indiquons par ailleurs qu'en août 2015 a été publié le rapport d'étude « From social media service to advertising network. A critical analysis of Facebook's Revised Policies and Terms » écrit par l'ICRI de la KU Leuven, le SMIT de la VUB et le COSIC de la KU Leuven.

3 Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 111 (somm.), note G. Dejemeppe. Cet arrêt est disponible en intégralité sur http://deeplinking.kluwer.nl/?param=00CCEC7E&cpid=WKNL-LTR-Nav2.

4 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit. Ce jugement est disponible en français en intégralité sur le site web de l'Autorité de protection des données. Voy. https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/jugement_facebook_16022018.pdf.

5 Sur cette affaire, voy. C. Fievet, L. Gérard, N. Gillard, M. Knockaert, A. Michel, J. Mont, K. Rosier, Th. Tombal et O. Vanreck, « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information », in *Chronique de jurisprudence en droit des technologies de l'information 2015-2017*, H. Jacquemin et Th. Tombal (coord.), *R.D.T.I.*, 2017, nos 68-69, pp. 129 à 132.

6 La cour d'appel de Bruxelles a relevé qu'il ne pouvait y avoir d'urgence en l'espèce puisque les pratiques de traçages comportementaux des personnes non affiliées à *Facebook* ont débuté en 2012. Pour plus de détails sur cet arrêt, voy. *Ibid.*, pp. 96 à 97, 99 à 100 et 129 à 130.

Le président de la CPVP[7] a dès lors décidé d'introduire une action au fond, devant le tribunal de première instance néerlandophone de Bruxelles, à l'égard des trois filiales du site de réseautage social. À son estime, à l'aide de cookies, pixels et autres modules sociaux, *Facebook* traite, chaque jour et de manière totalement illégale, les données liées aux habitudes de navigation des internautes en Belgique. À la différence de la procédure de référé dans laquelle la CPVP dénonçait uniquement les méthodes de traçage comportemental visant les internautes non inscrits, l'action au fond porte également sur le profilage des personnes possédant un compte *Facebook*. Par ailleurs, l'autorité de contrôle belge signale que le site de réseau social recourt désormais, aux côtés des cookies « datr » et des plug-ins sociaux, à des techniques supplémentaires pour suivre les habitudes de navigation des internautes : il en va ainsi des pixels et des cookies « c_user », « xs », « sb », « fr » et « lu »[8]. Dans cette procédure au fond, la CPVP reproche principalement à *Facebook* la mise en place de diverses technologies de traçage, sans information adéquate et sans obtention du consentement valable des personnes concernées, destinées à obtenir les informations nécessaires au profilage des internautes – tant membres que non membres du réseau social – à des fins de ciblage publicitaire[9].

La présente contribution est l'occasion de se pencher sur le premier jugement rendu au fond, en date du 16 février 2018, dans l'affaire des cookies *Facebook* par le tribunal de première instance néerlandophone de Bruxelles.

Dans un premier temps, nous nous intéressons au phénomène du suivi des comportements en ligne qui a vu le jour à l'aube du Web 2.0 ainsi qu'aux techniques utilisées par *Facebook* pour traquer les internautes (point II).

Dans un second et dernier temps, nous développons les questions juridiques soulevées en l'espèce et analysées par le tribunal de première instance néerlandophone de Bruxelles. Ainsi, après avoir fait écho à la question de la compétence internationale à l'égard des filiales américaine et irlandaise du réseau social en abordant tour à tour les règles de droit international public, le champ d'application territorial ainsi que les compétences dévolues aux autorités de contrôle nationales (point III), nous traitons des points relatifs à la protection des données à caractère personnel pertinents en l'espèce (point IV). Bien que la présente affaire ait été soumise au juge belge sous l'égide de l'ancienne directive 95/46/CE[10], nous prenons le parti de systématiquement mentionner les changements apportés par le Règlement général sur la protection des données (ci-après « R.G.P.D. ») sur les questions

7 Indiquons que Monsieur Willem Debeuckelaere a introduit l'action au fond « en sa qualité » de président de feu la Commission belge de la protection de la vie privée (« CPVP »).

8 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. nº 2016/153/A, inédit, point 5. Les finalités poursuivies par ces différents types de cookies sont exposées au point 6 du jugement. Les cookies « c_user »,« xs » et « sb » sont destinés à vérifier l'identité et les connexions des internautes inscrits sur *Facebook*, le cookie « datr » poursuit des finalités liées à la sécurité et à l'intégrité du réseau social, le cookie « fr » a des vocations de publicités ciblées et le cookie « lu » conserve le choix de l'internaute de rester connecté sur son compte *Facebook*.

9 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. nº 2016/153/A, inédit, point 7.

10 Ancienne directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281, 23 novembre 1995, pp. 31 et s.

tranchées par le tribunal pour mesurer son impact sur les points débattus[11].

II. COOKIES ET TRAÇAGE DES HABITUDES DE NAVIGATION DES INTERNAUTES

A. Le phénomène du suivi des comportements en ligne

Avec l'avènement du Web 2.0 et le développement des sociétés offrant des services en ligne, est apparu le phénomène du pistage des habitudes de navigation des internautes, notamment à des fins de ciblage publicitaire. Ce n'est en effet un secret pour personne : lorsque nous surfons sur le net, nous sommes constamment « épiés » par les sociétés en ligne afin de récolter nos préférences en termes de consommation. Nos données sont ainsi traitées pour nous proposer les biens ou les services les plus susceptibles de nous intéresser avec notamment, pour conséquence dans certains cas, outre le non-respect de notre droit fondamental au respect de la vie privée, une politique de prix discriminants.

Ce phénomène de traçage du comportement en ligne des internautes se base sur différentes techniques telles que les cookies[12], les modules sociaux[13] ou les pixels[14]. Précisons que, à l'origine, le recours aux cookies – anonymes la plupart du temps – était justifié par le bon déroulement des communications en ligne. Il s'agissait ainsi de données techniques essentielles à la communication ayant pour « rôle initial » d'« assurer une continuité dans les échanges »[15]. Par la suite, s'est dessinée une évolution dans l'usage des cookies en vue de mettre en œuvre des fonctionnalités inédites permettant la poursuite de finalités nouvelles telles que le profilage ou l'offre de publicités ciblées. Par ailleurs, outre le fait qu'ils contiennent de plus en plus d'informations personnelles, le passage au système d'adressage « IPv6 »[16] permet d'aisément lier les cookies sauvegardés à une adresse IP déterminée répondant ainsi à la notion de « donnée

11 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119/14, mai 2016.

12 Pour une explication en des termes clairs et simples du placement et du fonctionnement des cookies ainsi que des interactions entre navigateurs et serveurs, voy. Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 6.

13 Les « *social plug-ins* » ou « modules sociaux » sont des éléments fournis par *Facebook* aux propriétaires de pages web externes au réseau social afin de permettre aux internautes de diffuser les contenus de ces dernières sur *Facebook*. Il s'agit typiquement des boutons « j'aime » ou « partager ». Voy. Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 6.

14 Un pixel est un composant technique, invisible à l'œil nu, inséré dans le code informatique et fixé sur une page web. Il confère la possibilité aux propriétaires de sites externes d'obtenir des données sur leurs internautes. Les pixels peuvent être utilisés à des fins publicitaires en permettant ainsi de « montrer ultérieurement, sur Facebook, aux visiteurs [de sites web externes] des publicités ciblées ». Voy. Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 6.

15 CPVP, Recommandation d'initiative n° 01/2015 concernant l'utilisation des cookies, 4 février 2015, points 63 et 67 (annexe I « Définitions, contexte et considérations générales »).

16 Voy. sur ce point, *Ibid.*, point 18 (note 4) : dans ce système d'adressage, « chaque connexion se voit alors attribuer une adresse unique, avec un risque accru des possibilités d'identification des visiteurs ».

à caractère personnel »[17-18]. L'emploi des cookies offre dès lors des possibilités de stockage des paramétrages et des diverses informations détenues par les sites web, ouvrant la voie à d'éventuels traitements illicites de données à caractère personnel[19].

Ces pratiques controversées de suivi du comportement de navigation des internautes avaient déjà poussé la CPVP, à la suite du Groupe de travail « Article 29 »[20], à prendre une recommandation d'initiative concernant l'utilisation des cookies en février 2015[21]. S'en était dans la foulée suivie une recommandation d'initiative ciblant plus spécifiquement le réseau social *Facebook*[22].

B. Bref historique des pratiques mises en place par *Facebook*

Au cœur de l'affaire commentée, se retrouve justement cette politique controversée de cookies mise en place par le réseau social. Il convient d'indiquer que, entre 2015 et 2018, *Facebook* a, à plusieurs reprises, adapté ses pratiques concernant l'utilisation des cookies, pixels et modules sociaux ainsi que les termes de sa « politique cookies ».

Dans un premier temps, après avoir revisité la « bannière cookies »[23] s'affichant sur les pages

17 Constitue une donnée à caractère personnel, « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Voy. R.G.P.D., art. 4, 1°.

18 À cet égard, voy. R.G.P.D., cons. n° 30. Par ailleurs, indiquons que la Cour de justice de l'Union européenne a déjà eu l'occasion d'affirmer que les adresses IP peuvent constituer des données à caractère personnel. Voy. C.J.U.E., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14, EU:C:2016:779, §§ 36 à 48. Sur cet arrêt, voy. C. Fievet, L. Gérard, N. Gillard, M. Knockaert, A. Michel, J. Mont, K. Rosier, Th. Tombal et O. Vanreck, *op. cit.* (voy. note 5), pp. 103 à 104.

19 CPVP, Recommandation d'initiative n° 01/2015, *op. cit.* (voy. note 15), points 66 et 71: ainsi, « en plus d'un simple rôle technique, [le cookie] est de plus en plus utilisé comme support d'informations utiles à la transaction elle-même », accroissant par conséquent les risques pour la vie privée des internautes.

20 Groupe de travail « Article 29 », Document de travail n° 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies, adopté le 2 octobre 2013, WP 208. Ce document analyse les conditions, les modalités et les schémas de mise en œuvre du consentement pour l'installation et l'utilisation de cookies tant au sens de l'ancienne directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel que de la directive « vie privée et communications électroniques » 2002/58/CE.

21 CPVP, Recommandation d'initiative n° 01/2015, *op. cit.* (voy. note 15).

22 CPVP, Recommandation d'initiative n° 04/2015 concernant 1) Facebook, 2) les utilisateurs d'Internet et/ou de Facebook ainsi que 3) les utilisateurs et fournisseurs de services Facebook, en particulier les « plug-ins » sociaux, 13 mai 2015. Précisons que cette recommandation a ultérieurement été complétée en avril 2017, notamment au vu de plusieurs modifications de la politique cookies de *Facebook* ainsi que de ses conditions d'utilisation. Voy. CPVP, Recommandation n° 03/2017 complément à la recommandation d'initiative n° 04/2015 concernant 1) Facebook, 2) les utilisateurs d'Internet et/ou de Facebook ainsi que 3) les utilisateurs et fournisseurs de services Facebook, en particulier les « plug-ins » sociaux, 12 avril 2017.

23 Bannière cookies de *Facebook* en 2016: « Nous utilisons des cookies pour aider à personnaliser le contenu, ajuster et mesurer les publicités sur mesure et vous offrir une expérience plus sûre. En cliquant sur le site ou en le parcourant, vous nous autorisez à collecter des informations sur et en dehors de Facebook via les cookies. Pour plus d'informations, y compris sur le contrôle que vous pouvez exercer à cet égard <politique d'utilisation des cookies> ». Désormais, la bannière s'affichant lors de toute première visite sur le domaine *Facebook* est la suivante: « Nous utilisons des cookies pour personnaliser le contenu, vous proposer un contenu pertinent et offrir une expérience plus sûre. En cliquant sur le site ou en le parcourant, vous nous autorisez à collecter des informations via les cookies. Pour en savoir plus, notamment sur les dispositions prises sur la protection de

web du domaine facebook.com, *Facebook* a décidé de refuser, à toute personne non connectée ou non inscrite, l'accès aux pages du réseau social (profils personnels ou de personnalités publiques, pages de restaurants ou de magasins divers, etc.), à l'exception notamment de la page d'inscription. L'internaute était alors renvoyé vers une page informative décrivant la politique cookies ainsi que ses objectifs de « sécurité »[24]. Le géant du réseau social justifiait ce bouleversement dans l'expérience de navigation de l'internaute par le fait que les mesures ordonnées par l'ordonnance de référé le contraignait à « limiter [l']utilisation d'un outil de sécurité important, le cookie "datr" »[25]. Ce dernier est ainsi présenté comme un « outil de sécurité sophistiqué » destiné à « protéger » le compte des internautes inscrits en distinguant les « visites légitimes » sur le réseau social des « visites illégitimes »[26]. Sans l'instrument de sécurité qu'offre l'installation de ce cookie, *Facebook* décelait un « danger potentiel » dans toutes visites de ses pages internet d'internautes non connectés surfant depuis le territoire belge, raison pour laquelle ces pages leur étaient inaccessibles[27].

Dans un second temps, *Facebook* a élargi ses pratiques de traçage afin de suivre également les habitudes de navigation des internautes non-utilisateurs à des fins publicitaires, notamment via les pixels intégrés sur des pages web externes[28]. Dans une optique de transparence, le géant du réseau social a adapté sa politique cookies afin de fournir de plus amples informations sur les types de cookies qu'il utilise ainsi que sur leurs finalités[29]. Précisons que *Facebook* a par ailleurs renoncé à l'installation automatique des cookies dans certaines situations comme la modification de la langue d'affichage d'une page web ou la consultation de la politique cookies[30].

Dans un troisième et dernier temps, le géant américain, suite à la recommandation n° 04/2015, a proposé à ses utilisateurs un mécanisme d'*opt-out* aux publicités ciblées directement accessible dans les paramètres de leur compte personnel[31]. Néanmoins, la CPVP dénonce le fait que, même si un internaute a mis en œuvre la possibilité d'*opt-out* au ciblage publicitaire offerte par le réseau social, *Facebook* reçoit encore le cookie « fr » destiné à des fins publicitaires lorsque l'internaute navigue sur une page web dans laquelle est inséré un module social[32].

Rappelons que si à l'origine dans la procédure en référé la CPVP reprochait uniquement au réseau social de suivre les comportements en ligne des internautes non inscrits, l'autorité de contrôle belge élargit ensuite les griefs dans l'affaire commentée au profilage des internautes membres de *Facebook*. À cet égard, mentionnons la recommandation n° 03/2017

la vie privée, consultez la Politique d'utilisation des cookies ».

24 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 4.

25 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 4.

26 Parmi les visites considérées comme illégitimes, sont cités à titre exemplatif les profils de spammeurs, de hackers, de faux comptes ou d'internautes malintentionnés. Par ailleurs, *Facebook* précise également que le cookie « datr » permet d'éviter les éventuelles attaques techniques et rend la connexion des titulaires de compte plus rapide pour qu'ils soient capables d'« atteindre les personnes, photos et messages auxquels [ils tiennent], sans courir de risque au niveau des informations ». Voy. Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 4.

27 CPVP, Recommandation n° 03/2017, *op. cit.* (voy. note 22), point 19.

28 *Ibid.*, point 21.

29 *Ibid.*, point 21. Voy. aussi Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 6.

30 CPVP, Recommandation n° 03/2017, *op. cit.* (voy. note 22), points 23 et 38.

31 *Ibid.*, point 33.

32 *Ibid.*, point 34.

venant compléter la recommandation d'initiative n° 04/2015 dans laquelle la CPVP énumère les différentes techniques mises en œuvre par le réseau social pour profiler les personnes lorsqu'elles surfent sur le net sur des pages web en dehors du domaine facebook.com en deux catégories : d'une part, les internautes utilisateurs du réseau social (qu'ils soient connectés, déconnectés, désinscrits à l'offre de publicités ciblées ou encore qu'ils aient temporairement désactivé leur compte personnel) et, d'autre part, les internautes non utilisateurs de *Facebook*[33].

III. COMPÉTENCE DES JURIDICTIONS BELGES, LOI APPLICABLE ET AUTORITÉ DE CONTRÔLE

Dans le jugement commenté, le tribunal de première instance néerlandophone de Bruxelles se penche, dans un premier temps, sur la question controversée de la compétence qui a vivement animé le débat entre les parties dans les premiers volets de la saga judiciaire des « cookies *Facebook* ».

Pour rappel, après que le président du tribunal de première instance néerlandophone de Bruxelles[34] se soit déclaré compétent pour connaître du litige à l'égard des trois filiales de *Facebook* (*Facebook Inc.*, *Facebook Ireland Limited* et *Facebook Belgium SPRL*), la cour d'appel de Bruxelles[35] a réformé l'ordonnance de référé pour défaut de compétence internationale s'estimant dès lors seulement compétente à l'égard de l'entité belge du géant du réseau social[36].

Dans la décision commentée – qui rappelons-le traite pour la première fois de l'affaire au fond –, la CPVP demande au tribunal de se déclarer internationalement compétent pour connaître du litige à l'égard des filiales américaine et irlandaise. De son côté, *Facebook* conteste complètement la compétence de la CPVP. Il présente *Facebook Ireland Limited*[37] comme la seule cocontractante possible pour les internautes belges – et plus largement européens – et comme l'unique responsable du traitement de toute donnée à caractère personnel concernant les internautes de l'Union européenne[38]. Quant à la succursale belge, elle serait, aux yeux du réseau social, uniquement destinée à fournir un support en termes de « politique publique » pour le service *Facebook* et dépendrait alors directement de la maison mère (*Facebook Global Holdings LLC*)[39].

A. Règles de compétence applicables aux actions intentées par les autorités de contrôle

En l'espèce, puisque la présente action a été introduite « en vertu de son autorité publique », la CPVP argue que l'examen de la compétence internationale des tribunaux belges doit se faire, non pas à la lumière du droit privé international comme développé par la cour d'appel de Bruxelles, mais au regard des règles régissant le droit international public et, plus précisément, à l'aune du principe de

33 *Ibid.*, points 25 à 43.

34 Civ. Bruxelles (nl.) (réf.) (ord.), 9 novembre 2015, *R.D.T.I.*, 2016/1, n° 62, p. 91, note G. Dejemeppe.

35 Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 111 (somm.), note G. Dejemeppe.

36 Pour un commentaire et une analyse détaillée des questions de compétence et de droit applicable soulevées tant par l'ordonnance de référé que par l'arrêt de la cour d'appel, voy. G. Dejemeppe, « L'affaire *Facebook* : questions de procédure », note sous Civ. Bruxelles (nl.) (réf.) (ord.), 9 novembre 2015 et Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, pp. 113 à 126. Dans cette note d'observations, l'auteur explore les questions de compétence internationale et de loi applicable au litige, sous l'angle du droit international privé, en développant tour à tour les arguments du juge des référés et de la cour d'appel.

37 *Facebook* estime donc qu'est seule compétente l'autorité de contrôle irlandaise et que la présente procédure doit être soumise au droit irlandais.

38 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 2.

39 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 2.

territorialité[40]. Ainsi, à son estime, puisque les infractions reprochées au réseau social ont lieu et/ou sortent leurs effets en Belgique, que les personnes concernées et les appareils qu'elles utilisent sont présents sur le territoire belge et que la stratégie commerciale de *Facebook* vise également ce territoire, l'exigence de « liens substantiels suffisants » avec la Belgique est remplie[41].

Dans l'appréciation de sa compétence, le tribunal – se ralliant à la position défendue par C. Kuner[42] – déclare que, dans le domaine de la protection des données à caractère personnel, chaque affaire doit faire l'objet d'un examen *in concreto* afin de déterminer si elle relève du droit privé ou du droit public[43]. Dans cette optique, alors que le droit public régit les actions intentées par les autorités de contrôle nationales, les litiges – tant contractuels qu'extracontractuels – entre les sociétés offrant des services en ligne et les particuliers s'inscrivent dans une perspective de droit privé[44]. Ainsi, pour les actions intentées à l'égard d'un service de réseau social, les règles applicables à la détermination de la juridiction compétente dépendront des parties à l'action : d'une part, la juridiction compétente pour connaître des litiges opposant un réseau social à l'un de ses abonnés (contractuel) ou à un internaute non inscrit (extracontractuel) sera déterminée par le droit privé international et, d'autre part, les règles du droit international public détermineront la juridiction compétente pour les actions intentées par les organismes de l'État dans la limite de leurs compétences[45].

Considérant qu'en l'espèce la CPVP agit « en tant que pouvoir public dans le cadre des compétences qui lui sont octroyées en qualité "d'autorité de contrôle" nationale », le tribunal de première instance néerlandophone de Bruxelles examine sa compétence au regard du droit international public et s'éloigne dès lors du raisonnement tenu par la cour d'appel de Bruxelles[46]. Le tribunal de première instance néerlandophone de Bruxelles s'estime dès lors compétent pour connaître de l'affaire tant à l'égard de la filiale belge que des filiales irlandaise et américaine du groupe *Facebook*.

Pour ce faire, il analyse, d'une part, les compétences dévolues à la CPVP en tant qu'« autorité » au sens large du terme et, d'autre part, si cette dernière agit bel et bien en conformité avec les règles de juridiction du droit international public[47]. Par ailleurs, à l'instar des réflexions développées par la Cour de justice de l'Union européenne dans son arrêt *Weltimmo*[48], le tribunal souligne la distinction capitale entre les compétences conférées aux autorités de contrôle nationales et le champ d'application territorial des lois nationales relatives à la protection des données à caractère personnel et se penche sur leurs interactions[49].

40 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 10.

41 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 10. Notons que la CPVP invoque également la circonstance que la société *Facebook* possède un établissement physique en Belgique.

42 C. Kuner, « Data Protection Law and International Jurisdiction on the Internet (Part 1) », *International Journal of Law and Information Technology*, 2010/2, n° 18, pp. 176 à 193.

43 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 12.

44 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 12.

45 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 12.

46 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 12.

47 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 15.

48 C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, aff. C-230/14, EU:C:2015:639. Sur ce point, voy. *infra* « le champ d'application territorial ».

49 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 15.

Tout en donnant écho au raisonnement tenu par le tribunal, il nous semble primordial de consacrer quelques lignes à deux éléments clés en l'espèce : d'une part, le champ d'application territorial des règles relatives à la protection des données à caractère personnel et, d'autre part, les prérogatives des autorités nationales de contrôle. Par ailleurs, même si l'analyse en la présente affaire s'est déroulée sous l'égide de l'ancienne directive 95/46/CE[50], nous verrons quels impacts les changements introduits sur ces deux fronts par le R.G.P.D.[51] entré en application le 25 mai 2018 pourraient avoir sur le cas tranché si on les analysait sous l'angle de cette réglementation.

B. Le champ d'application territorial

Avant l'entrée en application du R.G.P.D., l'ancienne loi belge du 8 décembre 1992[52] prévoyait en son article 3*bis* deux critères de rattachement territorial. Le premier rendait la loi belge applicable en présence d'un traitement effectué « dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public »[53]. Le second visait la situation dans laquelle un responsable du traitement n'était pas établi « de manière permanente » dans l'Union européenne mais recourait « à des moyens automatisés ou non » situés en Belgique pour le traitement de données à caractère personnel[54].

Dans le cadre de la décision commentée, le premier critère relatif au traitement réalisé « dans le cadre des activités réelles et effectives d'un établissement du responsable du traitement » a animé le débat entre le réseau social et la CPVP. Dans son raisonnement, le tribunal de première instance néerlandophone de Bruxelles a commencé par rappeler la jurisprudence de la Cour de justice de l'Union européenne relative à l'interprétation à conférer à ce critère au sens de l'ancienne directive 95/46/CE[55]. Sans entrer dans les détails, précisons qu'en vertu de son arrêt *Google Spain*, la Cour de justice estime qu'un traitement de données à caractère personnel est « effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire d'un État membre » lorsqu'une multinationale crée une filiale en poursuivant un objectif de ventes d'espaces publicitaires aux habitants de cet État membre, activité intimement liée à l'activité principale de la multinationale et la rendant par ailleurs « économiquement rentable »[56]. De plus, dans ses arrêts *Weltimmo*

50 Ancienne directive 95/46/CE précitée.

51 Règlement (UE) 2016/679 précité.

52 Ancienne loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.

53 Ancien article 3*bis*, 1°, de l'ancienne loi du 8 décembre 1992 précitée.

54 Ancien article 3*bis*, 2°, de l'ancienne loi du 8 décembre 1992 précitée.

55 C.J.U.E. (GC), 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Espanola de Protección de Datos (AEPD) et Mario Costeja González*, aff. C-131/12, EU:C:2014:317 ; C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, aff. C-230/14, EU:C:2015:639 ; C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sarl*, aff. C-191/15, EU:C:2016:612. Sur ces trois arrêts, voy. respectivement pour l'arrêt *Google Spain* C. Burnet, M. Piron, B. Losdyck, O. Vanreck, J.-M. Van Gyseghem, E. Degrave, C. Gayrel, J. Herveg et K. Rosier, « Libertés et société de l'information », *R.D.T.I.*, 2015, nos 59-60, pp. 86 à 88 et pour les arrêts *Weltimmo* et *Verein* C. Fievet, L. Gérard, N. Gillard, M. Knockaert, A. Michel, J. Mont, K. Rosier, Th. Tombal et O. Vanreck, *op. cit.* (voy. note 5), pp. 97 à 99.

56 C.J.U.E. (GC), 13 mai 2014, *Google Spain* précité, points 55 et 56. Voy. également le point 60 de cet arrêt : « l'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publici-

et *Verein*, la Cour a également eu l'occasion de préciser que la notion d'établissement au sens de la directive « s'étend à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable »[57].

Appliquant les raisonnements développés par la Cour de justice en l'espèce, le tribunal réfute l'argument du réseau social selon lequel la filiale irlandaise aurait été instituée en qualité de responsable de tout traitement de données des internautes au sein de l'Union européenne au motif qu'au sens de la directive « le lieu d'établissement précis du responsable du traitement (…) n'est pas pertinent »[58]. En effet, pour appliquer la loi belge en l'espèce, il importe plutôt d'examiner si *Facebook* « exerce, au moyen d'une installation stable sur le territoire de la Belgique, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué, ou encore, si le responsable du traitement (…) procède au traitement des données concernées dans le cadre des activités d'un établissement situé en Belgique »[59].

En l'occurrence, il apparaît que la filiale belge du groupe *Facebook* exerce plusieurs activités publicitaires : aide à la filiale irlandaise pour la commercialisation des espaces publicitaires, supports aux publicitaires belges clients de la filiale irlandaise, contacts avec des sociétés belges notamment à des fins de ventes d'espaces publicitaires par *Facebook Ireland*, etc. Il en découle, aux yeux de la juridiction belge, que « le groupe *Facebook* dispose d'une installation stable en Belgique, *Facebook Belgium*, qui a sa propre personnalité morale et une activité effective, durable et réelle »[60]. Par ailleurs, le tribunal considère, à l'instar des développements de l'arrêt *Google Spain*, que les activités de la filiale belge sont étroitement et indissociablement liées à celles du groupe *Facebook* en ce qu'elles rendent le service de réseau social « économiquement rentable » et en ce que les traitements de données à caractère personnel effectués par le groupe *Facebook* à des fins de ciblage publicitaire « sont également le moyen par lequel l'établissement belge est en mesure d'exercer ses activités »[61]. Par conséquent, le site de réseau social exerce bel et bien une activité commerciale – en recourant notamment à des traitements de données à caractère personnel – dans le cadre des activités du responsable du traitement sur le territoire de la Belgique, rendant ainsi l'ancienne loi belge du 8 décembre 1992 applicable en l'espèce[62].

En ce qui concerne le champ d'application territorial, le R.G.P.D. apporte des modifica-

taires proposés par ce moteur et dont l'activité vise les habitants de cet État membre ». Dans le même sens, voy. également le point 41 de l'arrêt *Weltimmo* précité dans lequel la Cour de justice de l'Union européenne a précisé que : « l'article 4, paragraphe 1, sous a), directive 95/46 doit être interprété en ce sens qu'il permet l'application de la législation relative à la protection des données à caractère personnel d'un État membre autre que celui dans lequel le responsable du traitement de ces données est immatriculé, pour autant que celui-ci exerce, au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué ; afin de déterminer (…) si tel est le cas, la juridiction de renvoi peut, notamment, tenir compte du fait (…) que l'activité du responsable dudit traitement, dans le cadre de laquelle ce dernier a lieu, consiste dans l'exploitation de sites Internet d'annonces immobilières concernant des biens immobiliers situés sur le territoire de cet État membre et rédigés dans la langue de celui-ci et qu'elle est, par conséquent, principalement, voire entièrement, tournée vers ledit État membre (…) ».

57 C.J.U.E., 1er octobre 2015, *Weltimmo* précité, point 31 ; C.J.U.E., 28 juillet 2016, *Verein* précité, point 75.

58 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 19.

59 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 19.

60 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 19.

61 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 19.

62 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 19.

tions considérables par rapport à l'ancienne directive 95/46/CE, notamment en permettant désormais son application « à des acteurs situés bien loin des frontières de l'Union européenne »[63]. Par ailleurs, à la différence de la situation prévalant sous l'empire de la directive dans laquelle il était nécessaire de passer par l'étape de la détermination de la loi applicable grâce à des critères de rattachement, l'application du texte du R.G.P.D. est homogène – à l'exception des dispositions laissant encore une marge de manœuvre – dans tous les États membres[64]. Comme le précise alors C. de Terwangne, « le "rattachement" d'un traitement de données à un territoire national devient théoriquement inutile »[65].

L'article 3 du R.G.P.D. prévoit ainsi trois critères distincts d'application territoriale.

Premièrement, le R.G.P.D. s'applique à tout « traitement de données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union »[66]. Ce critère, repris de l'ancienne directive, a été légèrement remanié afin d'également viser les sous-traitants.

Deuxièmement, le R.G.P.D. vise également les traitements de données à caractère personnel concernant des personnes « se trouv[ant] sur le territoire de l'Union » par un responsable du traitement ou un sous-traitant non établi dans l'Union européenne dans deux hypothèses : d'une part, si le traitement est effectué dans le cadre d'offre gratuite ou payante de biens ou de services et, d'autre part, si le traitement poursuit une finalité de « suivi d'un comportement » qui s'est produit dans l'Union européenne[67]. L'on assiste dès lors avec le R.G.P.D. à un glissement du critère de l'ancienne directive relatif à la « localisation des moyens de traitement »[68] vers celui de la « localisation du public cible »[69].

Troisièmement et enfin, le R.G.P.D. instaure par ailleurs un critère d'application territoriale issu du droit international public. Les dispositions du texte européen s'appliqueront ainsi au traitement de données à caractère personnel réalisé par un responsable du traitement dont l'établissement se situe en dehors de l'Union européenne lorsque ce dernier se trouve « dans un lieu où le droit d'un État membre s'applique en vertu du droit international public »[70].

Il en résulte que, dans le cadre de l'affaire commentée, le nouveau champ d'application territorial instauré par le R.G.P.D. permettrait de couper court aux discussions relatives à la détermination de la loi applicable.

Par exemple, le fait qu'à l'estime de *Facebook* seulement l'une de ses trois filiales doive être considérée comme l'unique responsable du traitement dans l'affaire des « cookies *Facebook* » n'a que peu d'importance : dans les trois cas, qu'il s'agisse de l'américaine, de l'irlandaise ou de la belge, le réseau social devra respecter les dispositions du R.G.P.D. lorsqu'il effectue des traitements de données à caractère

63 C. de Terwangne, « Définitions clés et champ d'application du R.G.P.D. », in *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 59.

64 *Ibid.*, p. 76.

65 *Ibid.*, p. 76.

66 R.G.P.D., art. 3, paragraphe 1er. Précisons que les apports de la Cour de justice de l'Union européenne développés *supra* quant à cette notion de « traitement dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Union européenne » valent toujours sous l'égide du R.G.P.D.

67 R.G.P.D., art. 3, paragraphe 2, points a et b.

68 Ce critère s'appliquait notamment à l'enregistrement de cookies sur les terminaux des internautes situés au sein de l'Union européenne. Voy. à ce sujet, C. de Terwangne, « Définitions clés … », *op. cit.* (voy. note 63), p. 80.

69 *Ibid.*, pp. 80 à 81.

70 R.G.P.D., art. 3, paragraphe 3.

personnel dans le cadre des activités de ses établissements sur le territoire de l'Union européenne mais aussi lorsqu'il traite les données à caractère personnel de personnes se trouvant sur le territoire de l'Union même sans y être lui-même établi (traitement à des fins d'offre de services en ligne ou à des fins de suivi d'un comportement se produisant sur le territoire de l'Union européenne).

Même si, de toute évidence, les considérations émises par le tribunal de première instance néerlandophone de Bruxelles dans la décision commentée quant aux traitements effectués «dans le cadre des activités d'un établissement du responsable du traitement situé en Belgique» valent toujours en vertu du premier critère d'application territoriale du R.G.P.D., les autres critères permettent de rendre le R.G.P.D. applicable en simplifiant les débats…

En effet, en cas de doute sur le lieu d'établissement d'un responsable du traitement ou d'un sous-traitant au sein de l'Union européenne ou clairement confronté à un établissement hors de l'Union européenne, le simple fait que *Facebook Inc.* traite, à l'aide de cookies, pixels et autres modules sociaux, les données à caractère personnel d'internautes présents sur le territoire de la Belgique et suive ainsi leurs habitudes de navigation en ligne à des fins de ciblage publicitaire suffit à rendre le texte du R.G.P.D. applicable en vertu de son article 3, paragraphe 2, b). À cet égard, le considérant n° 24 du R.G.P.D. apporte des éclaircissements sur la notion de «suivi d'un comportement ayant eu lieu au sein de l'Union»: «afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur Internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit»[71]. À la lecture de ce considérant, force est de constater que les activités de suivi du comportement de navigation en ligne des internautes réalisées par *Facebook* en l'espèce rentrent clairement dans l'hypothèse visée à l'article 3, paragraphe 2, b), du R.G.P.D.

Par ailleurs, relevons également que les traitements de données à caractère personnel d'internautes surfant depuis la Belgique effectués par *Facebook* sont également susceptibles de se voir appliquer les dispositions du R.G.P.D. en vertu de l'article 3, paragraphe 2, a). En effet, ces traitements sont liés à l'offre d'un service en ligne de réseau social par *Facebook Inc.* aux internautes surfant depuis la Belgique.

C. Les compétences de la nouvelle «Autorité de protection des données»[72]

Auparavant, au niveau de l'Union européenne, les compétences des autorités nationales de contrôle indépendantes, veillant à la correcte application des dispositions en matière de protection des données à caractère personnel, étaient inscrites à l'article 28 de l'ancienne directive 95/46/CE qui laissait cependant une marge de manœuvre aux États membres. Ces dernières se voyaient notamment confier, outre leur mission de rendre des avis, des pouvoirs d'investigation, d'intervention et d'ester en justice ou de porter à la connaissance des autorités judiciaires toute violation

[71] R.G.P.D., cons. 24.

[72] Pour une réflexion et une analyse complète sur la réforme des autorités de contrôle et, plus précisément, de feu la CPVP devenue Autorité de protection des données, nous renvoyons le lecteur vers E. Degrave, «"L'autorité de contrôle: 'vues' de Bruxelles". Et que voit-on de Namur, vingt ans après?», in *Droit, normes et libertés dans le cybermonde. Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 581 à 597.

de la législation relative à la protection des données à caractère personnel[73]. Par ailleurs, le paragraphe 6 de cette disposition précisait qu'« indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3 »[74].

De son côté, l'ancienne loi du 8 décembre 1992 précisait la composition, le rôle, les pouvoirs et les missions de l'ancienne Commission de la protection de la vie privée belge. Elle était entre autres chargée de remettre des avis ou des recommandations, de traiter les plaintes qui lui étaient soumises et de dénoncer les éventuelles infractions en matière de traitement de données à caractère personnel au procureur du Roi[75]. Par ailleurs, – et c'est précisément la compétence exercée par la CPVP dans le jugement commenté et approuvée par le tribunal de première instance néerlandophone de Bruxelles en l'espèce – le président de la CPVP se voyait octroyer la possibilité de « soumettre au tribunal de première instance tout litige concernant l'application de la [loi] et de ses mesures d'exécution »[76].

Indiquons également que la CPVP a été instituée en Belgique en 1992, soit trois ans avant l'harmonisation des autorités de contrôle nationales par l'ancienne directive 95/46/CE. À cet égard, précisons que le législateur belge avait pris le parti de faire usage de la marge de manœuvre conférée par l'article 28 de l'ancienne directive 95/46/CE et n'avait pas pourvu la CPVP « des pouvoirs d'investigation et d'intervention organisés par la directive, ni du pouvoir d'amende »[77]. Il en découlait alors qu'en pratique la CPVP n'inspirait pas vraiment la crainte puisqu'elle se contentait majoritairement de jouer un rôle « d'organe d'avis et de conciliation », mettant ainsi en péril l'effectivité de son action…[78]

Toutefois, le R.G.P.D., ne laissant à l'inverse de la directive aucune marge d'appréciation aux États membres quant à l'étendue des pouvoirs des autorités nationales de contrôle, a nettement impacté l'autorité instituée en Belgique[79]. L'on assiste dès lors à un phénomène de baisse de « l'intervention *a priori* » des autorités de contrôle en faveur de « l'intervention *a poste-*

73 Ancienne directive 95/46/CE précitée, article 28, paragraphe 3.

74 Ancienne directive 95/46/CE précitée, article 28, paragraphe 6. Sur l'interaction entre la loi applicable et les compétences des autorités nationales de contrôle, voy. C.J.U.E., 1er octobre 2015, *Weltimmo* précité, point 60 : « (…) Dans l'hypothèse où l'autorité de contrôle d'un État membre saisie de plaintes, conformément à l'article 28, paragraphe 4, de la directive 95/46/CE, parviendrait à la conclusion que le droit applicable au traitement des données à caractère personnel concernées est non pas le droit de cet État membre, mais celui d'un autre État membre, l'article 28, paragraphes 1, 3 et 6, de cette directive doit être interprété en ce sens que cette autorité de contrôle ne pourrait exercer les pouvoirs effectifs d'interventions qui lui ont été conférés conformément à l'article 28, paragraphe 3, de ladite directive que sur le territoire de l'État membre dont elle relève. Partant, elle ne saurait infliger de sanctions sur la base du droit de cet État membre au responsable du traitement de ces données qui n'est pas établi sur ce territoire, mais devrait, en application de l'article 28, paragraphe 6, de la même directive, demander à l'autorité de contrôle relevant de l'État membre dont le droit est applicable d'intervenir ».

75 Anciens articles 29 à 32 de l'ancienne loi du 8 décembre 1992 précitée.

76 Ancien article 32, paragraphe 3 de l'ancienne loi du 8 décembre 1992 précitée. Précisons qu'il apparaît que la CPVP n'a recouru qu'une seule et unique fois à cette possibilité de porter une affaire devant le tribunal de première instance, en ce qui concerne justement l'affaire des « cookies *Facebook* ». Voy. sur ce point, E. Degrave, « "L'autorité de contrôle : 'vues' de Bruxelles" … », *op. cit.* (voy. note 72), p. 585.

77 *Ibid.*, p. 584.

78 *Ibid.*, p. 585.

79 *Ibid.*, pp. 584 à 585. Indiquons en effet que les législateurs d'autres États membres avaient déjà, suite à la transposition de l'ancienne directive 95/46/CE, conféré des compétences administratives à leur autorité nationale de contrôle leur permettant de directement ordonner des mesures ou imposer des amendes administratives, ce qui n'était pas le cas pour la CPVP en Belgique.

riori»[80]. Ainsi, avec le nouvel article 58 du R.G.P.D., les autorités de contrôle se voient entre autres investies de pouvoirs d'enquête et d'adoption de mesures correctrices[81].

S'en est alors suivi en Belgique une réforme de la CPVP laissant désormais place à l'«Autorité de protection des données» (ci-après «APD») avec la nouvelle loi du 3 décembre 2017 portant création de l'Autorité de protection des données[82-83]. L'APD n'est donc plus un simple organe d'avis mais devient une réelle «autorité de contrôle et de sanction» pouvant mener des enquêtes avec diverses mesures via son service d'inspection[84], ordonner toute une série de mesures et infliger des sanctions allant de l'avertissement ou de la réprimande à l'astreinte ou à l'amende administrative[85] par le biais de sa chambre contentieuse[86]. À côté de ces pouvoirs les plus souvent mis en exergue, l'article 6 de la loi du 3 décembre 2017 maintient le pouvoir pour l'APD «de porter toute infraction aux principes fondamentaux de la protection des données à caractère personnel […] à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice en vue de voir appliquer ces principes fondamentaux»[87].

Par conséquent, cela signifie que, confrontée à une affaire telle que celle des «cookies *Facebook*», l'APD n'aura pas à se contenter de dénoncer une éventuelle violation de la loi aux cours et tribunaux ou d'ester en justice, mais elle pourrait directement ordonner la mise en conformité des traitements effectués par le réseau social voire la suppression des données à caractère personnel détenues ainsi qu'imposer une amende administrative éventuellement assortie d'une astreinte… Dans une telle hypothèse, *Facebook* disposerait d'une possibilité de recours quant à la décision prise par la chambre contentieuse de l'APD à son encontre devant la cour des marchés (section de la cour d'appel de Bruxelles)[88].

D. Arrêt rendu par la cour d'appel de Bruxelles

Les développements qui précèdent sont à nuancer. En effet, suite à sa condamnation par le jugement commenté, le réseau social a interjeté appel devant la cour d'appel de Bruxelles qui vient tout juste de rendre son arrêt le 8 mai 2019.

Bien que cet arrêt ne fasse pas l'objet du présent commentaire, mentionnons que la juridiction d'appel s'est écartée du raisonnement tenu par les juges du fond dans l'affaire commentée. À l'instar de son homologue ayant réformé l'ordonnance de référé en date du 29 juin 2016[89], la cour d'appel de Bruxelles s'est estimée uniquement compétente à l'égard de la filiale belge de *Facebook* et donc sans compétence internationale envers les succursales irlandaise et américaine[90].

80 *Ibid.*, p. 584. L'auteure cite à titre d'exemples la suppression des obligations de déclaration préalable des traitements à l'autorité de contrôle et son remplacement par l'obligation de tenue d'un registre des activités de traitement ou encore les pouvoirs d'enquête et d'adoption de mesures correctrices.

81 *Ibid.*, p. 584.

82 *Ibid.*, pp. 585 et 586.

83 Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018. Voy. spécialement l'article 3.

84 Voy. les articles 64 et suivants de la loi du 3 décembre 2017 précitée.

85 Sur quelques précisions et considérations prospectives sur ce nouveau pouvoir d'amende conféré à l'APD, nous renvoyons le lecteur à la contribution d'Élise Degrave, voy. E. Degrave, «"L'autorité de contrôle : 'vues' de Bruxelles" … », *op. cit.* (voy. note 72), pp. 586 à 588.

86 Voy. art. 100 de la loi du 3 décembre 2017 précitée. Voy. également les articles 101 à 107. Voy. notamment les mesures que peut ordonner la chambre contentieuse de l'APD précisées aux articles 95 et 100 de la loi du 3 décembre 2017 précitée.

87 Loi du 3 décembre 2017 précitée, art. 6.

88 Voy. article 108 de la loi du 3 décembre 2017 précitée.

89 Bruxelles (18e ch. N), 29 juin 2016, *R.D.T.I.*, 2016/1, n° 62, p. 111 (somm.), note G. Dejemeppe.

90 Bruxelles, 8 mai 2019, R.G. n° 2018/AR/410, inédit. Le dispositif de cet arrêt uniquement est disponible en néerlandais sur le site de l'APD. Voy. https://www.

Néanmoins, avant de se prononcer sur le fond de l'affaire, la cour d'appel de Bruxelles pose toute une série de questions préjudicielles à la Cour de justice de l'Union européenne afin de s'assurer que, suite à l'entrée en application du R.G.P.D., l'APD soit en mesure de poursuivre la procédure engagée par l'ancienne CPVP à l'encontre de *Facebook*[91]. En effet, le R.G.P.D. prévoit désormais le mécanisme du « guichet unique »[92] destiné à améliorer la coopération entre les autorités de contrôle des différents États membres. La cour d'appel de Bruxelles s'interroge alors sur les éventuelles conséquences d'un tel mécanisme sur le pouvoir des autorités de contrôle d'ester en justice ou d'informer les autorités judiciaires de toute violation aux dispositions du R.G.P.D. en vertu du paragraphe 5 de son article 58[93].

IV. VIOLATION PAR *FACEBOOK* DES RÈGLES IMPOSÉES PAR LA LÉGISLATION RELATIVE À LA PROTECTION DES DONNÉES

De toute évidence, les pratiques mises en œuvre par *Facebook* pour suivre – grâce aux cookies, aux modules sociaux et aux pixels – le comportement en ligne des internautes surfant sur le web depuis la Belgique, afin de leur envoyer des publicités ciblées en fonction de leurs habitudes de navigation, doivent se conformer tant à la législation relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (en l'espèce, l'ancienne loi du 8 décembre 1992[94]) qu'à l'article 129 de la loi du 13 juin 2005 relative aux communications électroniques[95].

Selon la CPVP, ces pratiques, qu'elles visent des personnes inscrites ou non sur *Facebook*, violent le cadre légal applicable en l'espèce. En effet, l'autorité de contrôle belge estime que le réseau social n'a pas obtenu le consentement valable des internautes (tant sur le plan de l'ancienne loi du 8 décembre 1992 sur que le plan de l'article 129 de la loi du 13 juin 2005), n'a pas respecté les principes applicables aux traitements de données à caractère personnel et n'a pas adéquatement informé les internautes. Dans le jugement commenté, le tribunal de première instance néerlandophone de Bruxelles a dès lors été amené à se prononcer sur ces différents aspects.

gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Dispositief_arrest.pdf.

91 Pour plus d'informations sur cette affaire, voy. Autorité de protection des données, « La cour d'appel de Bruxelles réfère l'affaire *Facebook* à la Cour de justice de l'Union européenne », le 8 mai 2019, disponible sur https://www.autoriteprotectiondonnees.be/news/la-cour-dappel-de-bruxelles-refere-laffaire-facebook-a-la-cour-de-justice-de-lunion, consulté le 18 juin 2019. Pour la formulation des diverses questions préjudicielles posées par la cour d'appel de Bruxelles à la Cour de justice de l'Union européenne, voy. https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Dispositief_arrest.pdf.

92 Voy. R.G.P.D., cons. nos 127 et 128.

93 Voy. Autorité de protection des données, *op. cit.* (voy. note 91).

94 Ancienne loi du 8 décembre 1992 précitée.

95 Loi du 13 juin 2005 relative aux communications électroniques, art. 129, paragraphe 1er : « Le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un abonné ou d'un utilisateur est autorisé uniquement à condition que 1° l'abonné ou l'utilisation concerné reçoive conformément aux conditions fixées dans la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, des informations claires et précises concernant les objectifs du traitement et ses droits sur la base de la loi du 8 décembre 1992 ; 2° l'abonné ou l'utilisateur final ait donné son consentement après avoir été informé conformément aux dispositions visées au point 1° ». *Facebook* se doit en effet d'également respecter cette disposition puisqu'il stocke des informations dans l'équipement terminal des internautes (inscrits ou non sur le réseau social), notamment à l'aide de cookies, dans l'objectif de pouvoir accéder ultérieurement à ces informations lorsque ces derniers surfent sur des pages web extérieures au domaine *Facebook*.

A. Le consentement des internautes

Tout d'abord, pour le placement des cookies et les traitements de données à caractère personnel effectués, le géant du réseau social estime obtenir un consentement valable de la part des utilisateurs – inscrits ou non – grâce à la « bannière cookies »[96] s'affichant lors de la toute première visite sur une page web appartenant au domaine *Facebook*. Il considère que cette dernière permet aux internautes d'être conscients, qu'en cliquant sur le site ou en le parcourant, ils consentent à la « politique cookies » du réseau social pour deux finalités précises : d'une part, une finalité publicitaire (personnalisation du contenu et offre d'un contenu pertinent) et, d'autre part, une finalité de sécurité (offre d'une expérience plus sûre)[97].

Selon l'ancienne loi du 8 décembre 1992, un consentement valable devait répondre à quatre conditions cumulatives : le caractère indubitable, le caractère libre, le caractère spécifique ainsi que le caractère informé[98].

Précisons tout de même que, par rapport à l'ancienne directive 95/46/CE, le R.G.P.D. a le mérite de renforcer la qualité du consentement requis, notamment par le remplacement de l'exigence du caractère indubitable par le caractère « univoque » du consentement permettant de « manifester la volonté de la personne concernée par une déclaration ou un acte positif clair »[99-100]. Par ailleurs, rappelons que, pour le stockage d'informations ainsi que pour l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un abonné ou d'un utilisateur, l'article 129 de la loi relative aux communications électroniques exige, outre l'information de la personne concernée, que le responsable du traitement obtienne le consentement de l'utilisateur final ou de l'abonné[101]. L'installation de cookies et la consultation ultérieure des informations qu'ils contiennent – à l'exception de nécessités purement techniques – rentrant dans le cadre de cette disposition, le consen-

96 Pour rappel, la bannière s'affichant désormais lors de toute première visite sur le domaine *Facebook* est la suivante : « Nous utilisons des cookies pour personnaliser le contenu, vous proposer un contenu pertinent et offrir une expérience plus sûre. En cliquant sur le site ou en le parcourant, vous nous autorisez à collecter des informations via les cookies. Pour en savoir plus, notamment sur les dispositions prises sur la protection de la vie privée, consultez la Politique d'utilisation des cookies ».

97 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 31.

98 Sur ce point, voy. anciens articles 1er, paragraphe 8 et 5 de l'ancienne loi du 8 décembre 1992 précitée. Selon l'article 5, a), « le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants : a) lorsque la personne concernée a indubitablement donné son consentement ». Par ailleurs, l'article 1er, paragraphe 8 définissait le consentement comme « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Voy. également l'avis de l'ancien Groupe de travail « Article 29 » sur la définition du consentement qui contient de nombreuses précisions et explications sur les quatre conditions cumulatives d'un consentement valable au sens de l'ancienne directive 95/46/CE : Groupe de travail « Article 29 », avis n° 15/2011 sur la définition du consentement, adoptée le 13 juillet 2011, WP 187.

99 Voy. C. de Terwangne, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », in *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, pp. 121 et 122. Mentionnons que l'article 4, 11°, du R.G.P.D. entend par consentement de la personne concernée « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

100 Pour une analyse complète et détaillée des changements apportés par le R.G.P.D. quant au consentement de la personne concernée, nous nous permettons de renvoyer le lecteur à la contribution de Cécile de Terwangne sur le sujet. Voy. C. de Terwangne, « Les principes … », *op. cit.* (voy. note 99), pp. 120 à 131.

101 Loi du 13 juin 2005 relative aux communications électroniques, art. 129, paragraphe 1er.

tement des internautes est indéniablement requis pour de telles opérations.

Dans l'affaire commentée, le tribunal procède à une analyse fouillée[102] en appliquant au cas d'espèce les conditions cumulatives entourant le consentement valable de l'internaute, sous l'égide de l'ancienne directive 95/46/CE, à l'utilisation de technologies permettant le suivi de ses habitudes de navigation à des fins sécuritaires et publicitaires.

Le caractère indubitable du consentement – à tout le moins lorsque les internautes (inscrits ou non) surfent sur le domaine *Facebook*[103] – ne semble pas provoquer de discussions particulières. En l'espèce, le tribunal considère, d'une part, que les personnes membres du réseau social ont donné un consentement indubitable au placement de cookies lors de leur inscription et, d'autre part, que les personnes non inscrites qui continuent à surfer sur les pages web du domaine *Facebook* après l'affichage de la bannière cookies lors de leur première visite consentent également de manière indubitable au placement de cookies[104]. Si le caractère indubitable semble respecté en l'espèce, il en va par contre autrement des autres conditions à remplir pour obtenir un consentement valable.

Premièrement, selon tribunal de première instance néerlandophone de Bruxelles, le consentement des internautes n'est pas informé. Il se rallie à la position de la CPVP selon laquelle les informations fournies par *Facebook* aux internautes sur diverses pages web du réseau social ne sont pas suffisamment compréhensibles et accessibles. La juridiction relève que ni la bannière cookies (première couche d'information) ni les politiques d'utilisation des cookies et des données (deuxième et troisième couches d'information) n'explicitent assez clairement les finalités précises de la collecte des données à caractère personnel[105]. Par ailleurs, les internautes surfant sur des pages web externes au domaine du réseau social mais contenant des modules sociaux *Facebook* ne reçoivent pas davantage de renseignements clairs sur les types de données collectées afin de tracer leurs habitudes de navigation en ligne[106]. Le tribunal relève encore l'absence d'information relative à l'existence des droits d'accès et de rectification ainsi qu'à la durée de conservation des données collectées par *Facebook* grâce aux cookies, pixels et modules sociaux[107]. Par la suite, le tribunal donne raison à la CPVP quant au fait que le géant américain communique des informations trompeuses sur les hypothèses dans lesquelles il installe des cookies et sur les différents types de cookies utilisés listés dans la politique d'utilisation des cookies (notamment, l'absence de la finalité publicitaire poursuivie par le cookie « c_user »)[108].

102 Pour les développements complets, nous renvoyons le lecteur aux points 32 à 35 du jugement commenté. Voy. Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, points 32 à 35.

103 Le caractère indubitable du consentement signifie que la manière dont le responsable du traitement obtient le consentement de la personne concernée au traitement de ses données à caractère personnel ne doit entraîner aucun doute possible sur son intention réelle de consentir audit traitement. Voy. Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 34.

104 Voy. Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 34.

105 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 32.

106 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 32. Selon le tribunal, en prenant connaissance de la politique d'utilisation des données, il est en effet impossible pour l'internaute moyen de se rendre clairement compte que *Facebook* « traque » ses habitudes de navigation sur le net (hors domaine *Facebook*) pour lui proposer des publicités ciblées.

107 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 32.

108 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 32.

Deuxièmement, le tribunal suit l'argument de la CPVP qui dénonçait l'absence d'un consentement libre pour les personnes non inscrites sur *Facebook*. Aux yeux de l'autorité de contrôle belge, si ces personnes ne veulent pas consentir à l'installation de cookies, leur seule alternative est de fermer la page web malgré les conséquences négatives qu'elles subissent de leur refus de consentir[109]. En effet, outre le fait que ces internautes ne pourront pas bénéficier du service en ligne offert par le réseau social, ils seront plus fondamentalement privés de l'accès à toute une série de renseignements relatifs à des entreprises privées qui disposent uniquement de pages *Facebook* et donc d'aucun site web propre « concurrent » permettant de consulter ailleurs que sur *Facebook* ces informations[110]. Le tribunal de première instance néerlandophone de Bruxelles précise, qu'au vu de la position dominante mondiale du géant américain dans le domaine des réseaux sociaux, l'on peut attendre de *Facebook* qu'elle soit en mesure d'offrir des contenus web aux internautes sans nécessiter que ces derniers consentent « à l'installation de tous les cookies »[111].

Troisièmement et enfin, la juridiction en vient alors à regretter le caractère non spécifique des consentements recueillis par *Facebook* pour l'installation de cookies sur les équipements terminaux des internautes, qu'ils soient membres ou non du réseau social. En effet, ces derniers sont contraints de consentir au placement de la totalité des cookies et sont dans l'impossibilité d'uniquement exprimer un consentement pour un ou certains cookies, ce qui est d'autant plus problématique puisque les internautes ne sont pas clairement au fait de la collecte de leurs données à caractère personnel lorsqu'ils surfent sur des pages extérieures au domaine *Facebook*[112]. Par ailleurs, le tribunal souligne que le réseau social collecte toujours les informations relatives au comportement de navigation des internautes malgré l'activation du mécanisme d'*opt-out* pour les publicités ciblées, ce qui n'est donc pas de nature à remettre en cause l'analyse du caractère spécifique du consentement[113].

Par conséquent, il découle de l'ensemble de l'analyse opérée par le tribunal de première instance néerlandophone de Bruxelles que *Facebook* n'obtient pas le consentement valable des internautes, qu'ils soient ou non membres du réseau social, pour suivre leurs habitudes de navigation en ligne.

B. Examen des autres hypothèses de licéité des traitements

Ensuite, le tribunal de première instance néerlandophone de Bruxelles examine la possibilité de légitimer les traitements de données à

109 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 34.

110 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 34.

111 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 34.

112 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 34. Indiquons que l'ancien Groupe de travail « Article 29 » précise dans son avis 15/2011 que le responsable du traitement peut se fonder sur un consentement unique pour légitimer plusieurs traitements à condition que la personne concernée puisse raisonnablement s'attendre à l'ensemble de tels traitements de données à caractère personnel. En l'espèce, le tribunal estime que les internautes ne peuvent pas raisonnablement s'attendre aux traitements de leurs données lorsqu'ils surfent sur le web en dehors des pages appartenant au réseau social. Dès lors, un consentement unique ne peut être perçu comme valable en l'espèce…

113 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 34. En effet, la possibilité d'*opt-out* vise au final uniquement l'utilisation ultérieure des informations relatives aux habitudes de navigation des internautes mais pas leur collecte initiale. Par ailleurs, indiquons que l'ancien Groupe de travail « Article 29 » exige dans son avis n° 15/2011 que le consentement de l'internaute soit obtenu avant toute installation de cookies sur son équipement terminal. Voy. Groupe de travail « Article 29 », *op. cit.* (voy. note 98).

caractère personnel effectués par *Facebook* sur base des autres hypothèses de licéité de l'article 5 de l'ancienne loi du 8 décembre 1992.

Le réseau social arguait en effet que l'installation et la lecture ultérieure de cookies sur les équipements terminaux des internautes était triplement légitime. Premièrement, pour les personnes inscrites, *Facebook* estimait que le traitement des données les concernant était nécessaire pour l'exécution du contrat de fourniture du service en ligne de réseau social. Dès lors, certains cookies («c_user», «xs» et «lu») assureraient le fonctionnement correct et efficace du service en ligne offert aux internautes. Deuxièmement, le géant américain faisait valoir que le recours aux cookies susceptibles d'enregistrer des données à caractère personnel était nécessaire à la réalisation de ses intérêts légitimes. Troisièmement et enfin, le réseau social invoquait également le respect de l'obligation légale de sécurisation des données à caractère personnel qui lui est imposée en vertu du paragraphe 4 de l'article 16 de l'ancienne loi du 8 décembre 1992[114]. Ainsi, l'utilisation des cookies de sécurité «datr» et «sb» aurait été primordiale pour assurer la protection efficace des informations personnelles de millions d'internautes transitant par le réseau social[115].

Le tribunal va estimer que, bien que la sécurisation du service en ligne constitue bel et bien un intérêt légitime pour *Facebook*, les traitements réalisés pour ce faire ne sont pas nécessaires à son accomplissement. En effet, le recours aux modules sociaux sur les pages web externes au domaine *Facebook*, afin de procéder à la collecte systématique des données à caractère personnel d'internautes (membres ou non du réseau social), n'est pas nécessaire pour sécuriser les données à caractère personnel[116].

C. Non-respect des principes clés du traitement

Le tribunal de première instance néerlandophone de Bruxelles relève enfin que *Facebook* a violé plusieurs des principes clés devant guider les traitements de données à caractère personnel autrefois listés à l'article 4 de l'ancienne loi du 8 décembre 1992: les principes de loyauté, de finalité et de proportionnalité[117].

114 Article 16, paragraphe 4, de l'ancienne loi du 8 décembre 1992 précitée: «Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels». Indiquons que le président du tribunal de première instance néerlandophone de Bruxelles avait déjà rejeté cette hypothèse de licéité de traitement fondée sur l'obligation légale imposant au responsable du traitement de prendre les mesures techniques et organisationnelles nécessaires à la protection contre tout problème de sécurité et d'intégrité des données à caractère personnel dans l'ordonnance de référé rendue le 9 novembre 2015. Le président considérait en effet qu'une telle obligation légale ne s'imposait à *Facebook* qu'à partir du moment où elle pouvait légitimer ses traitements de données à caractère personnel, c'est-à-dire uniquement en présence d'un motif d'admissibilité du traitement valable. Pour plus de détails, C. Fievet, L. Gérard, N. Gillard, M. Knockaert, A. Michel, J. Mont, K. Rosier, Th. Tombal et O. Vanreck, *op. cit.* (voy. note 5), pp. 131 à 132.

115 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 35.

116 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 36. L'objectif de sécurité pourrait être atteint sans ce traitement de données à caractère personnel en recourant à un moyen moins attentatoire aux droits et libertés de la personne concernée. Relevons que le tribunal applique le même raisonnement à l'hypothèse de licéité relative à la nécessité pour l'exécution d'un contrat auquel la personne concernée est partie.

117 Depuis le 25 mai 2018, voy. R.G.P.D., art. 5 et 6.

En ce qui concerne le principe de loyauté, outre l'absence d'un motif d'admissibilité valable pour légitimer les traitements, le tribunal déplore le manque de loyauté du géant américain envers les millions d'internautes surfant depuis le territoire belge. La loyauté, intrinsèquement liée à l'exigence de transparence, signifie que le responsable du traitement ne peut recourir à la tromperie et doit clairement informer les personnes concernées[118]. Ainsi, « l'idée est d'annoncer loyalement aux personnes concernées le sort qui attend leurs données »[119]. Or, le tribunal regrette tant le manque d'accessibilité aux informations[120] que leur caractère obscur, ce qui *de facto* impacte le caractère loyal des traitements de données[121]. En effet, lorsque les internautes surfent sur des pages web en dehors du domaine *Facebook*, le réseau social « place et collecte, sans en informer suffisamment les internautes, systématiquement et sans qu'ils ne posent d'actes, des cookies et autres données, à des fins publicitaires »[122]. Par ailleurs, le tribunal indique que Facebook trompe les attentes raisonnables des internautes qui ont activé la possibilité d'*opt-out* aux publicités ciblées puisqu'il ne cesse de suivre leurs habitudes de navigation en ligne à des fins publicitaires[123].

À l'égard du principe de proportionnalité, le tribunal estime que, au vu des finalités poursuivies par *Facebook*, la collecte des données à caractère personnel des internautes à l'aide de cookies et de modules sociaux est dans de nombreuses situations non nécessaire. Comme mesures superfétatoires, le tribunal cite par exemple la lecture systématique de cookies de sécurité qui peut être facilement contournée par des internautes malveillants avec un minimum de connaissances techniques. Par ailleurs, dans la balance des intérêts à opérer, la juridiction estime que les droits et libertés des internautes l'emportent indéniablement sur les intérêts du réseau social en raison du caractère particulièrement attentatoire des techniques mises en place pour suivre les comportements en ligne tant au niveau du type de données, de l'ampleur du profilage que de la durée de conservation des cookies[124].

D. Sanction prononcée à l'encontre de *Facebook*

Accueillant l'intégralité des arguments avancés par la CPVP, le tribunal de première instance néerlandophone de Bruxelles décide de condamner le géant américain pour violation de l'ancienne loi du 8 décembre 1992 et de l'article 129 de la loi du 13 juin 2005. En effet, il ressort du raisonnement du tribunal que, pour ses activités de suivi du comportement en ligne des internautes (inscrits ou non), *Facebook* n'obtient aucun consentement valable, manque à ses obligations d'information et surtout viole le principe de loyauté.

Le tribunal ordonne une série de mesures accompagnée d'une astreinte de 250.000 euros par jour de retard à l'encontre des trois filiales (belge, irlandaise et américaine) de *Facebook* :

– la cessation tant de l'installation que de la collecte des cookies sur les équipements terminaux des internautes aussi longtemps qu'elle ne respectera pas les exigences de

118 C. DE TERWANGNE, « Les principes … », *op. cit.* (voy. note 99), pp. 90 et 91.

119 *Ibid.*, p. 91.

120 Sur ce point, le tribunal renvoie au raisonnement tenu lors de l'analyse du caractère informé du consentement (manque d'explicitation des finalités précises de la collecte, du type de données collectées, de l'information relative aux droits de la personne concernée, de la durée de conservation des données, etc.).

121 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 36.

122 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 36.

123 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 36.

124 Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n° 2016/153/A, inédit, point 36.

la législation relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;
- la cessation de ses pratiques déloyales consistant à offrir des informations susceptibles de tromper l'internaute sur les mécanismes de gestion de l'utilisation des cookies ; et
- la suppression de l'intégralité des données à caractère personnel des internautes surfant depuis la Belgique collectées illégalement[125].

V. CONCLUSION

Au fil du temps, *Facebook* a développé un arsenal de techniques permettant de suivre les comportements en ligne des personnes surfant sur le net : cookies en tout genre, modules sociaux ou encore pixels. Bien que ces derniers puissent parfois s'avérer nécessaires à l'utilisation du service en ligne ou à la sécurisation de l'expérience de l'internaute sur le réseau social, leur usage s'avère bien plus discutable lorsqu'ils ont à dessein le profilage des individus dans l'objectif de leur proposer des publicités ciblées. Quoi qu'il en soit, le recours à ces techniques impliquant des traitements de données à caractère personnel, le géant américain se doit de respecter la législation relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

À cet égard, le jugement commenté a donné l'occasion aux juridictions belges de se prononcer pour la première fois au fond sur les pratiques du réseau social. Alors qu'au départ la CPVP dénonçait uniquement les violations à l'égard des internautes non inscrits, l'autorité de contrôle belge a par la suite élargi ses griefs pour également viser les membres de *Facebook*. Contrairement à l'arrêt d'appel réformant l'ordonnance de référé, le tribunal de première instance néerlandophone de Bruxelles, appliquant les règles du droit international public, s'est déclaré compétent pour connaître de l'affaire à l'égard des filiales américaine, irlandaise et belge du géant américain. Dans son jugement rendu en date du 16 février 2018, le tribunal a entièrement donné raison à la CPVP et a condamné *Facebook* pour non-respect de l'ancienne loi du 8 décembre 1992 et de l'article 129 de la loi du 13 juin 2005. Ainsi, le réseau social se voit principalement reprocher trois violations. Premièrement, il n'obtient aucun consentement valable de la part des internautes (inscrits ou non) et ne peut par ailleurs légitimer les traitements réalisés sur aucun autre motif d'admissibilité. Deuxièmement, il n'offre pas une information suffisamment claire, précise et accessible aux personnes concernées quant à la collecte et aux traitements de leurs données à caractère personnel, surtout lorsqu'elles visitent des pages web en dehors du domaine facebook.com. Troisièmement, le tribunal regrette le caractère déloyal des pratiques mises en œuvre par le réseau social : outre le manque de transparence quant au sort réservé aux données, *Facebook* trompe les attentes raisonnables des internautes en continuant à collecter les données relatives à leurs habitudes de navigation malgré l'activation du mécanisme d'*opt-out* aux publicités ciblées. Les enseignements du jugement rendu par le tribunal de première instance néerlandophone de Bruxelles permettent de rendre compte de la sévérité des exigences du droit à la protection des données, notamment en ce qui concerne les conditions entourant la validité d'un consentement ainsi que l'équilibre à ménager entre l'intérêt légitime du réseau social souhaitant recourir aux cookies et les intérêts, libertés et droits fondamentaux des personnes concernées. *Facebook* doit ainsi prêter attention au respect de ces exigences strictes, à défaut de quoi son modèle écono-

[125] Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. nº 2016/153/A, inédit, point 39.

mique risquerait de s'en trouver remis en cause…

Par ailleurs, nous avons eu l'occasion de relever le double impact du R.G.P.D. sur une affaire telle que celle des cookies *Facebook*. D'une part, depuis le 25 mai 2018, les dispositions du R.G.P.D. ont vocation à s'appliquer aux responsables du traitement établis en dehors de l'Union européenne si le public cible est localisé au sein de l'Union. Ainsi, peu importe la filiale concernée, *Facebook* devra se soumettre au R.G.P.D. pour le suivi des habitudes de navigation des personnes surfant sur Internet depuis le territoire belge. Il en ira de même pour les traitements effectués dans le cadre de l'offre du service de réseau social. En ce qui concerne la problématique du profilage des internautes localisés au sein de l'Union grâce aux informations récoltées via les cookies et autres techniques de traçage, saluons les apports du R.G.P.D. En effet, pour ce type de traitements poursuivant indubitablement une finalité de « suivi d'un comportement », *Facebook* se doit, selon l'article 3, paragraphe 2, b), de se soumettre à la nouvelle réglementation européenne. D'autre part, le R.G.P.D. a également entraîné une conséquente réforme de l'autorité de contrôle en Belgique. À l'inverse de l'ancienne CPVP, l'APD a les compétences nécessaires pour directement ordonner des mesures contraignantes à *Facebook*. Dès lors, dans une affaire telle que celle commentée en l'espèce, l'APD pourrait toujours ester en justice mais aura par ailleurs la possibilité de se montrer plus répressive via sa chambre contentieuse en ordonnant directement au réseau social de se conformer au R.G.P.D. ou de supprimer les données collectées illégalement voire même en lui infligeant une amende administrative.

Quoi qu'il en soit, les juridictions belges n'ont pas encore livré le mot de la fin de la saga judiciaire de l'affaire des cookies *Facebook*. En effet, après sa condamnation par le jugement commenté, le réseau social a interjeté appel auprès de la cour d'appel de Bruxelles qui vient tout juste de rendre son arrêt le 8 mai 2019. Contrairement au tribunal de première instance néerlandophone de Bruxelles, la cour se déclare incompétente pour connaître du litige à l'égard de *Facebook Inc.* et de *Facebook Ireland* (succursales américaine et irlandaise). En outre, avant de se prononcer sur le fond à l'encontre de *Facebook Belgium*, la cour d'appel adresse une série de questions préjudicielles à la Cour de justice de l'Union européenne concernant l'impact du R.G.P.D. sur la possibilité pour l'APD de poursuivre la procédure initiée par la CPVP, reportant ainsi le dénouement de l'affaire de quelques mois supplémentaires…

Alejandra Michel